Assignment C
Tasks 1-4 from Handout

Prepared for
Dr. Steven D. Zink, Ph.D.
2004 Winter Institute
Faculty in Doctoral Program
Nova Southeastern University

Prepared by
Derek J. Sedlack
Doctoral Student, Nova Southeastern University
School of Computer and Information Sciences

October 24, 2004

Task 1

Given the latency of information policy formulation in the United States, was the rapid enactment of the recent, sweeping laws regarding electronic data and record-keeping, "overkill" or "overdue"? Justify your response with specific examples.

It is very difficult to say that canonical epitaphs presented to legislature that produce popular laws are either "overkill" or "overdue", when in fact they are both. Anderson, Bikson, Law, and Mitchell (1995) note that Email has been around for over four decades, but the swath of laws that have inundated the industry in the past five years is astonishing. The issue surrounding electronic data and record-keeping is not if the laws are justified, but how to properly implement and apply them without creating a simple headdress to placate the public after the outcry over corporate implosions. Understanding the motivation behind many of these bills is complex, but a fundamental understanding of Washington polls may provide insight. As Davis (2003, p. 1) said, "you just need to go back to the headlines."

Conte (2002) found that 600 bills were designed specifically to crack down on identity theft, probably as a direct result of the staggering financial losses that American companies are experiencing from a "victimless crime." A September 2003 FTC report noted costs businesses and financial institutions almost $48 billion dollars during 2002 alone. None of the 600 bills, however, addressed the release of medical information, purposefully or not (Garfinkel, 2000). Garfinkel found that even the most public and influential figures have had medical information leaked into the public. In fact, some instances may have been deliberate, yet no laws exist that categorize this behavior as punishable. Redefining undesirable actions as criminal behavior may perhaps stem the tide of illegal activities being produced by the accessibility and ease of use created by electronic commerce. The free use of information to steal identities, or purposefully divulge information that might have been kept private if not for the availability provided by technology does force legislature to act. Should congress wait until there is a victim to push through legislature?

Senator Hatch (2004) produced a bill in response to the estimated billions in losses the recording companies and artists were loosing because of illegally replicated and distributed music over the Internet. MP3 technology was created in 1987 by a group of researchers at the Fraunhofer Institut, led by Karlheinz Brandenburg, a specialist in mathematics and electronics and was adopted by the Industry Standards Organization (ISO) in 1992 as the MPEG-1 standard. The MP3 music encoding, derived from MPEG compression algorithms, received a US patent in 1996 and only two years later the use of this method became so popular with entrepreneurs who created programs to rip songs from CDs that Fraunhofer started to enforce the patent rights (Bellis, n.d.). The compression method allowed the storage of roughly ten times the number of songs available on a single CD purchased from a retail outlet. Only when the industry began seeing a perceived loss of sales to this "new" technology did they ask legislature to intervene, but students already believed that no laws were being broken when they "shared" music with friends or even made it available globally over the Internet.

The US General Accounting Office (USGAO) (2003) described the difficult challenges they are facing attempting to permanently preserve documents and records of historical interest

and additionally managing a massive number of obsolete or deteriorating storage media. The USGOA oversees each agency's responsibility for the management of its own records, even when the USGOA has not scheduled or even address the management of more recent forms of media like Adobe formatted portable or hypertext documents.

Permanent methods of document storage have not been developed, CDROMs only have a shelf life of one year, so how is a small business expected to "ensure that records maintained in such systems [electronic recordkeeping systems] can be correlated with related records on paper, microform, or other media," much less a conglomerate with over 50,000 employees (NARA, 2001, 1234.22). It would be virtually impossible to keep track of paper documents in Germany that correspond to digital documents in Kansas, or PowerPoint presentations that were included. The tumultuous economic situations created by Enron and WorldCom's rapid implosion should have caused enough concern in Congress to create laws to stem the tide of future catastrophes. It is also reasonable to believe that unsecured documents and health records would also cause rise to bills that protect individuals from individuals additionally. But creating them without providing companies with reasonable steps to completion or expectations for compliance can only hurt the U.S. economy further. While the sweeping laws are needed, they must be ratified so that any hope of compliance is not only within grasp, a majority of business must be able to reasonably comply.

Task 2

Several recent regulatory issuances have indicated that backfiles of emails must be retained for a specified period of years, depending on the nature of the business. How realistic are these requirements?

Taking the best-case scenario for the business, a business with 25 employees or less that does not depend on Internet connectivity or electronic commerce and communications to survive. This business would probably accumulate 10-20 emails per employee, per day from both professional and personal contacts. Table 1 illustrates the potential issues surrounding storage requirements. Assuming the current storage costs, ~$1 per Gigabyte fixed disk storage according to http://www.pricewatch.com, a company would fill a 100Gb drive with email along in roughly

Average Email (Kb)	Total # / Day	Total Employees	Storage Requirement (Kb)
40	15	25	15,000
50	25	50	62,000
60	50	500	1,500,000
70	75	5000	26,250,000
80	100	10000	80,000,000

[Table 1. Matrix of possible Email storage potentials in different corporate environments]

10 days of normal activity, not counting attachments such as PowerPoint attachments, compressed data files, or images that would make the storage requirement considerably larger. Companies that are graphic intensive, or rely on electronic communications for a majority of their business could expect a significant increase in storage requirements over the estimated potentials from Table 1, increasing their overall costs of short-term storage to a level around $4,000 yearly. Tolson (2002) estimated 9,000,000,000Kb per day for 3,000 employees receiving 60 emails of 50,000Kb in size, totaling 321,865 Gigabytes storage or $321,865 with growth year over year. Using a Network Attached Storage solution would be more expensive in physical cost, ~$4 a Gigabyte plus the additional cost of hardware and management. Digital Video Disks average ~$9 a Gigabyte, but provide a much more stable method of storage than server hard disk or network attached disks.

Using any of these methods with a wide variety of variables in both storage requirements and storage methods increase fixed long-term costs by unbelievable numbers. Perhaps these laws are being pushed by the IT storage industry since the 2000 bubble produced softer markets. CDROMs and DVDs are not permanent solutions and the laws of physics dictate that any media that is created using magnetism or light has an inherent limitation of degrading properties. Alternative methods are being investigated, but are not currently available, even as laws predicate that some form of permanent archival become integrated into business processes in the near future. The NARA require clearly established chains of accessibility, but does not propose a method of sorting important email that must be saved from SPAM or irrelevant communications.

How would you approach the task of complying?

The first step in compliance is the development of a plan and formal process, even if the timeframe exceeds regulatory issuance. Communicating processes and procedures to responsible parties creates a consistent, repeatable process that construes intent and will help even the most bureaucratic corporations establish a path of change that can be modified to accommodate any instituted requirements. The USGAO (2003) itself acknowledges that most of the electronic records have not been scheduled for archival and the evolving software and hardware requirements and the complexity of electronic records pose extremely challenging planning requirements on everyone attempting to comply with storage and archival legislature. Assigning priority in itself requires the development of new processes along with AD (analog to digital) conversions of paper, hand-written, or faxed documents. Trying to correlate these diverse medium would require very sophisticated databases even for those companies that are not technology intensive or driven. Understanding the heterogeneity in business, the rapidly changing technology, and the sheer volume of digital information that companies encounter daily requires a delicate balance between creating laws that are enforceable and those that are successful.

Task 3

Draft a privacy statement for your organization's Web site. If your organization already has such a statement, how would you modify the policy to improve it based on the principles of privacy that you have learned in class and in your readings? Be specific and provide sample language.

Since I maintain only a rudimentary formal education in legality and I probably click far to quickly through End-User-Agreements, I will post my companies privacy statement with suggestions noted through change tracking built-in to the Word product.

Citrix Privacy Statement

Information Collection

Citrix deems our customer's privacy a central issue of Internet use. Citrix attempts to have reasonable measures in place to assure the anonymity of visitors to the Citrix web site to help them shop quickly and efficiently. Citrix feels as part of responsible disclosure that Citrix web site users are aware of what information is being logged and how that information is used.

To ensure the most pleasant and useful online experience, Citrix maintains and improves site quality and integrity through the logging of IP addresses (the Internet Protocol addresses of computers) that are not linked to personally identifiable information. This log is an industry standard method of reporting to statistically find out which parts of our web site are visited and how long visitors spend there. Additionally, we log the type of browser and operating system used during the online experience to ensure maximum compatibility.

Deleted: ,

Deleted: are logged

Deleted: W

Deleted: also

Deleted: you are using

Deleted: We do not link IP addresses to personally identifiable information.

Like many other commercial web sites, the Citrix web site may use a standard technology called a "cookie" to collect information about how you use the site. Cookies were originally designed to help a web site distinguish a user's browser as a previous visitor and thus save and remember any preferences that may have been set while the user was browsing the site. A cookie enhances the user's visit by securely storing personalized home pages, a user ID and password, identify which parts of the Citrix site are most important to customers, or keep track of "shopping cart" selections. A cookie cannot retrieve any other data from your hard drive, pass on computer viruses, or capture your e-mail address unless the user is specifically prompted. It is possible to set your browser to inform you when a cookie is being placed, modified, or removed — this way, you have the opportunity to decide whether to accept the cookie. Click here [provide hyperlink] to read instructions on how to set Internet Explorer version xxx or Netscape version xxx to inform cookie usage. Citrix is dedicated to ensuring that our customers navigate our Internet web site and knowledge base comfortably and confidently in compliance with United States laws and regulations.

Deleted: is a small string of text that a web site can send to your browser.

Deleted: Currently, web sites use cookies to enhance the user's visit; in general, cookies can securely store a user's ID and password, personalize home pages, identify which parts of a site have been visited or keep track of selections in a "shopping cart."

At times we may request that you voluntarily supply us with personal information, such as your e-mail address, for the purposes of correspondance, site registeration, making a purchase, entering a sweepstakes, registering a new product, or participating in an online survey.

Deleted: such as

Deleted: ing with us

Deleted: ing at a site

Information Use

Citrix is committed to customer privacy. When you supply Citrix with personal information, we may use the information to develop better products and services or use the information, sharing it only with our most trusted business partners, to serve you with new product information, savings, services and offers would probably be of specific interest to you.

Citrix is a multi-national corporation and follows the rules and procedures required by law regarding the transmission of personal information between countries.

Deleted: your

Deleted: learn more about you so that we can

Deleted: inform you about

Deleted: s

Deleted: that may be of

Deleted:

Declining E-mail Offers

Although most customers appreciate receiving notice of valuable opportunities, we recognize the importance provided by choices. At any time after receiving an e-mail offer from Citrix, you may request to discontinue receiving these offers. All e-mail offers that you receive from Citrix will tell you how to decline, or "opt-out" of further e-mail offers. Our trusted partners may have different policies.

Deleted: tell us they

Deleted: these

Deleted: of

Deleted: ing you with

Children

Citrix's product ad campaigns and marketing materials are designed with the family in mind and may be viewed by children, however, data received from children would not help enhance our professional relationship. Citrix encourages parents and guardians to spend time online with their children, explain Citrix' privacy commitment. and to participate in the interactive activities offered on the sites their children visit. No information is requested, should be submitted to, or posted at, Citrix's web site by visitors under 18 years of age without the consent of their parent or guardian.

Deleted: While

Deleted: we do not wish to receive

Deleted:

Citrix System Inc.'s privacy statement is subject to change at any time and without notice.

Task 4

Given growing popular concern over citizen privacy, should the U.S. government adopt, in totality, the principles behind the European Commission Privacy Directive? Why or why not?

The U.S. government should adopt, in totality, the principles behind the European Commission Privacy Directive for a number of reasons including: better protection for the largest service oriented country in the world, a clean inability of corporations to govern themselves, the ability to transact with the European community, and to provide leadership in shrinking global barriers that will soon disappear with respect to corporate boundaries.

While business schools scuttle to include ethics classes in their core curricula and the legal compliance profession may have had another banner year, Krawiec (2003) noted that only 25% of Americans believe most corporate executives are honest and corporations are not internally monitoring illicit activities when it is in their best interest to find loopholes for forget to follow proper procedures. "Negotiated governance," or internal conduct codes and compliance programs, appear to countermand published legal models that would suggest otherwise, providing under-deter business misconduct and an inundation of expensive internal compliance structures (Krawiec, 2003).

Ila Swan (2003), the California representative for the Association for the Protection of the Elderly and Board Member of Hospice Patients Alliance, posted a huge number of corporate settlements and acknowledgements of executive guilt on their web site that include: Johns Hopkins University misleading the government into granting $2.6 million more than lawfully entitled, Stony Brook Hospital returning $850,000 for Medicare fraud that included double billed pharmaceuticals, and Abbott Laboratories, Inc. agreeing to $600 million in fines over a criminal investigation that defrauded Medicare and Medicaid over a nine year period by over-reporting sales figures. If the Medicare and Medicaid programs that are supposed to protect our retirees is being defrauded of what appears to be billions of dollars a year, how can one expect powerful corporations like Abbott to comply with non-criminal privacy programs within the United States let alone through the outsourcing of such services?

Information privacy is an oxymoron when related to health care as U.S. Representative Nydia Velázquez found out after her medical records were faxed to a national publication that intended to run a front-page story on the dishonest, but not illegally received documents for the sole purpose of inhibiting her run at public office (Garfinkel, 2000). The release of healthcare information is not criminal, even if intentional and malicious in nature. And, since the information is factual, it cannot be deem slanderously unlawful. European laws require companies to register their databases even before they begin operations and collect personal information. The U.S. does not even monitor the massive databases currently compiled by Internet information gatherers like Doubleclick and Gator. The U.S. government Office of the Federal Compliance Commissioner published an Information Sheet 6 in 2001 regarding Security and Personal Information Protection stating, "National Privacy Principle (NPP) 4.1 provides that an organization (sic) must take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised (sic) access, modification or disclosure." Amazingly, printed on the final sheet is the following statement, "Information sheets are advisory only and are not legally binding" even while the Privacy Act of 1998 information is binding.

U.S. companies dealing with European counterparts promise to protect their consumer's personal information under the 2000 Safe Harbor framework, but with rampant disregard for current American policies and recommendations, how can Europeans, or other nations trust that American companies are truly complying with their most sensitive information? If the outsourcing of personal information is not illegal in the U.S. and Europe does not have agreements with India, China, or other outsourcing capitals, does that make the U.S. company Safe Harbor compliant, or not? If the United States hopes to become a leader in the service industry, or even compete on the same level as global players, they will have to adopt more stringent information compliance laws or even some more rigorous to prove that the privacy of information is of concern and will be protected.

Bibliography

Anderson, R. H., Bikson, T. K., Law, S. A., & Mitchell, B. M. (1995). *Universal Access to E-Mail: Feasibility and Societal Implications*. Santa Monica, CA: Rand Corporation.

Bellis, M. (n.d.). The history of MP3: Fraunhofer Gesellschaft and MP3. About.com. Retrieved from the World Wide Web on September 29, 2004 from http://inventors.about.com/od/mstartinventions/a/MPThree.htm

Conte, C. (2002, May). Getting to know you. *Governing*, pp. 46-50.

Cook, J. S., & Cook, L. L. (2004). Compliance with data management laws. *Social, Ethical and Policy Implications of Information Technology*. In L. L. Brennan & V. E. Johnson, chapter 15, 251-273. Hershey, PA: Information Science Publishing.

Davis, J. B. (2003, February). Sorting out Sarbanes-Oxley. *ABAJournal, 89*, 44-49.

Federal Trade Commission (FTC). (September, 2003). FTC releases survey of identity theft in U.S. 27.3 million victims in past 5 Years, billions in losses for businesses and consumers. *Federal Trade Commission for the Consumer*. Retrieved from the World Wide Web on October 12, 2004 from http://www.ftc.gov/opa/2003/09/idtheft.htm

Garfinkel. S. (2000). *Database Nation: The Death of Privacy in the 21st Century*. Cambridge, MA: O'Reilly and Associates.

Gaudin, S. (1999, December 27). The perils of privacy [risks of not developing policy]. *Network World*, 81-84.

Hatch, O. (2004). Hatch introduces bill to stop inducement of children to commit crime. Retrieved from the World Wide Web on October 2, 2004 from http://hatch.senate.gov/index.cfm?FuseAction=PressReleases.Detail&PressRelease_id=1083&Month=6&Year=2004&IsTextOnly=True

Hammitt, H. (1997, November). Privacy trumps access, and it ain't cheap. *Government Technology,* 18.

Hammitt, H. (1998, June). A constitutional right of informational privacy. *Government Technology,* 22.

Ila Swan (2003). Reports on fraud, government corruption & failures that result in suffering, wrongful deaths. Retrieved on September 22, 2004 from the World Wide Web from http://www.ilaswan.org/reports-articles-fraud-corruption-7-2004.html

Kieler, M., & West, M. J. (2004). Digital orphans: Technology's wayward children. *Social, Ethical and Policy Implications of Information Technology*. In L. L. Brennan & V. E.

Johnson, chapter 14, pp. 234-250. Hershey, PA: Information Science Publishing.

Krawiec, K. D. (2003). Cosmetic compliance and the failure of negotiated governance. *Washington University Law Quarterly, 81*, 487-544.

Margulius, D. L. (2004, February 9). Hazardous waste: How discarded hardware can hurt you. *Infoworld*, 43-46.

Rosen, J. (2001, December). Privacy, reconsidered. *CIO Insight*

Tolson, B. (2002, September). Controlling the flood: a look at email storage and management challenges - Automated Storage Management. LookSmart Find Articles. Retrieved on August 25, 2004 from the World Wide Web from http://www.findarticles.com/p/articles/mi_m0BRZ/is_9_22/ai_101679024

Valente, K. (2002, January). Is privacy no longer a priority? *Intelligent Enterprise*, pp. 48-49.

Worthen, B. (2003, April 15). What to do when Uncle Sam wants your data. *CIO*, pp. 56-66.

U.S. General Accounting Office (USGAO). (2003, July). *Management and Preservation Poses Challenges*. (GAO-03-936T). Washington: The Agency. Retrieved on October 12, 2004 from the World Wide Web from http://www.gao.gov/new.items/d03936t.pdf

U. S. National Archives and Records Administration (NARA). (2001). *Creation and use of text documents*. Records Management, subchapter B, part 1234. Retrieved on October 12, 2004 from the World Wide Web from http://www.archives.gov/about_us/regulations/part_1234.html